AO 93 (Rev. 11/13) Search and Seizure Warrant

AUSA: Timothy Wyse Telephone: (313) 226-9144
Special Agent: Michael Bertrand (FBI) Telephone: (313) 802-2688

UNITED STATES DISTRICT COURT

for the
Eastern District of Michigan

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* INFORMATION ASSOCIATED WITH: IP ADDRESS 212.71.235.148 STORED AT PREMISES CONTROLLED BY LINODE, LLC.	)	Case No. 19-mc-51360-4

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of Michigan.
(identify the person or describe the property to be searched and give its location):

See ATTACHMENT A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See ATTACHMENT B, violations of: 18 U.S.C. § 1028A ,18 U.S.C. § 1030 (aggravated identity theft, fraud and related activity in connection with computers) and 18 U.S.C. § 1343 (wire fraud).

YOU ARE COMMANDED to execute this warrant on or before June 15, 2023 *(not to exceed 14 days)*
☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the presiding United States Magistrate Judge on duty.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*
☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: June 1, 2023 4:59 pm

Judge's signature

City and state: Detroit, Michigan Hon. David R. Grand U. S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
19-mc-51360-4	6/2/2023 11:11 AM	LINODE WEB PORTAL

Inventory made in the presence of :

SA ANDY SCZYGIELSKI

Inventory of the property taken and name of any person(s) seized:

ELECTRONIC DATA PERTAINING TO SUBJECT SERVER

SHA384SUM_DUPE-1673450670-LINODE410721-79-82200404.img.BZ2.TXT
SHA384SUM-DUPE-1673450670-LINODE410721-79-82200405.img.BZ2.TXT
LEGAL-2712.PDF
SHA384SUM_DUPE-1673450670-LINODE410721-79-82200404.img.BZ2
SHA384SUM-DUPE-1673450670-LINODE410721-79-82200405.img.BZ2

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 8/2/2023

Executing officer's signature

SPECIAL AGENT MICHAEL BERTRAND

Printed name and title

ATTACHMENT A

Property to be Searched

This warrant applies to information associated with the server corresponding to the domain mandarincc.ru ("SUBJECT SERVER") that is stored at premises owned, maintained, controlled, or operated by Linode, LLC, a company headquartered at 329 E. Jimmie Leeds Rd. Ste A, Galloway, NJ 08205, namely information associated with mandarincc.ru located at IP address 212.71.235.148 from November 15 to November 17, 2022. This includes any and all data preserved in response to the Preservation of Records request sent to Linode regarding mandarincc.ru at 212.71.235.148 sent on January 3, 2023, and receiving Linode request reference number LEGAL-2323.

ATTACHMENT B

Information to be disclosed by Linode, LLC. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any images, snapshots, messages, records, files, logs, or information that have been deleted but are still available to the Provider, or otherwise preserved and retained by the Provider – the Provider is required to disclose the following information to the government with respect to the SUBJECT SERVER described in Attachment A.

1. All information previously preserved by way of Linode reference number LEGAL-2323 in response to the government's preservation request sent on January 3, 2023;
2. All files, databases, and other content information pertaining to the SUBJECT SERVER stored on behalf of its subscriber(s) and user(s), including
    a. All volatile memory used by virtualized and physical computers;
    b. SSH, FTP or similar logs showing connections related to the SUBJECT SERVER, and any other transactional information,

including records of session times and durations, log files, dates and times of connection, methods of connection, and ports;

c. Email accounts and the contents thereof, associated with the SUBJECT SERVER;

d. All forensic copies and snapshots of the contents of the SUBJECT SERVER described in Attachment A; information pertaining to the tool and process used to create forensic copy(ies); a log of the process; verification of the process; a record of who created the copy(ies), when the copy was created, and where each copy was created, including the person's name, title, contact number, and address;

3. All records and information, including passwords, encryption keys, and other access devices, that may be necessary to access the information associated with the SUBJECT SERVER;

4. Records related to how and when the server(s) associated with the SUBJECT SERVER were accessed or used including

a. All historical netflow logs relating to the SUBJECT SERVER described in Attachment A;

b. All full package capture ("PCAP") records relating to the SUBJECT SERVER described in Attachment A;

5. All records of other subscriber information regarding the account(s) associated with the SUBJECT SERVER described in Attachment A, to include

    a. Full name(s),

    b. Physical address(es),

    c. Telephone numbers and other identifiers,

    d. Records of session times and durations,

    e. The date on which the account was created,

    f. The length of service,

    g. The types of services utilized,

    h. The IP address used to register the account,

    i. Log-in IP addresses associated with session times and dates, account status,

    j. Alternate email addresses provided during registration,

    k. Method of connection,

    l. Log files,

    m. Means and source of payment (including full credit card and bank account numbers, bitcoin addresses, and other cryptocurrency payment information);

6. Subscriber information of user accounts known by the Provider to be linked to the subscriber by shared user data such as the subscriber's primary email, SMS, recovery email, secondary email, method of payment, serialized device, or provider cookie;
7. Device information associated with devices that accessed the SUBJECT SERVER
8. All records pertaining to communications between the Provider and any persons regarding the SUBJECT SERVER described in Attachment A, including contacts with support services and records of actions taken;
9. All notes, findings, and supporting documentation regarding the SUBJECT SERVER described in Attachment A.

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

ATTACHMENT C

Information to be seized by the government

All information described above in Attachment B that constitutes fruits, evidence, and instrumentalities of violations of 18 U.S.C. § 1028A, 18 U.S.C. § 1030, and 18 U.S.C. § 1343, involving the SUBJECT SERVER listed in Attachment A, information pertaining to the following matters:

1. All information described above in Attachment B above that constitutes evidence, contraband, fruits, or instrumentalities of criminal violations of 18 U.S.C. § 1028A ,18 U.S.C. § 1030 (fraud and related activity in connection with computers) and 18 U.S.C. § 1343 (wire fraud), namely:
    a. Information relating to who created, accessed, or used the SUBJECT SERVER, including records about their identities and whereabouts;
    b. Evidence indicating how and when the SUBJECT SERVER was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the account user(s);
    c. Evidence indicating how the SUBJECT SERVER was used, to determine its use in matters relating to a scheme or artifice to defraud or to access victim information without authorization;

d. Information relating to communications between any email address, moniker, or social networking account associated with the SUBJECT SERVER and any other computers or accounts that involve discussions of cyber-attacks, the compromise of computers, servers, and/or networks, the sale of stolen credit card information, as well as any communications showing the capabilities of persons engaged in computer intrusions;

e. Records and information relating to transactions involving virtual currencies or cryptocurrencies, including Bitcoin;

f. Contact information of the administrator(s) or co-conspirators;

g. Information relating to who created, accessed, or used the SUBJECT SERVER; and

h. All communications indicating the identity of the user(s) of the SUBJECT SERVER, including records that help reveal the user's/users' whereabouts.

2. Information concerning the establishment and operation of mandarincc.ru, including:

a. Information concerning mandarincc.ru's customers and victims;

b. Communications, discussions, or information relating to mandarincc.ru and the unlawful buying, selling and use of credit card information;

c. The creation of new domains, purchasing of domain infrastructure, and contact with the hosting company;

d. How and when the server was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and the account holder;

e. How and when co-conspirators may have assisted with the administration of mandarincc.ru;

f. Evidence of where the victim information originated from;

g. The owner's or owners' state of mind as it relates to the crimes under investigation; and

h. The identity of the person(s) who communicated with the hosting company about matters relating to a scheme or artifice to defraud or to access victim information without authorization, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records, and information disclosed pursuant to this warrant

in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.